REMARKS/ARGUMENTS

This paper is being submitted in response to the Non-Final Office Action dated January 31, 2005, having a shortened statutory period set to expire April 31, 2005, wherein:

Claims 1-16 were previously pending; and

Claims 1-16 were rejected.

After careful consideration of the Examiner's rejections in the above-identified Office Action, Applicants have canceled claims 1-16 without prejudice or disclaimer of the subject matter recited therein and submitted new claims 17-34 for consideration. Applicants respectfully submit that new claims 17-34 more clearly characterize embodiments of Applicants' invention and are distinguishable from the cited references of record. Consequently, claims 17-34 are currently pending in the above-identified patent application. Applicants submit that no new matter has been added by this amendment and request reconsideration of all pending claims in light of the amendments and remarks made herein.

Claim Rejections under 35 U.S.C. § 102

In the present Office Action, claims 1-16 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,175,924, issued to Arnold (hereinafter, "***Arnold***"). Although the Examiner's rejections have been rendered moot by the cancellation of previously-pending claims 1-16 and while not conceding that the Examiner's cited references qualify as prior art but rather in the interest of expediting prosecution, Applicants respectfully disagree with the Examiner's rejections and have therefore elected to traverse the rejections as applied to Applicants' currently pending claim as follows. Applicants reserve the right, for example in a continuation application, to establish that one or more of the Examiner's cited reference do not qualify as prior art with respect to the invention embodiments claimed in the above-identified application.

Applicants' Claims

Applicants' previously pending claim 1 (now canceled without prejudice or disclaimer of the subject matter recited therein) recited a method for generating a self-verifying certificate. More specifically, Applicants' previously-pending claim 1 recited separate master and target public keys ("establishing a master key pair including a master private key and a master public key...supplying a target public key"), an authentication code ("prompting a user for an authentication code"), and the generation of certificate only in response to a correct entry of the authentication code ("generating a self-verifying certificate utilizing said target public key and said master key pair only in response to a correct entry of said authentication code") (Applicants' claim 1, emphasis supplied).

Applicants' currently-pending claim 17 (as newly submitted herein) similarly recites a method for employing a digital certificate. More specifically, Applicants' claim 17 recites a master key pair and a target key pair including distinct first and second public keys ("storing a master key pair... wherein said master key pair comprises a first private key and a first public key...said digital certificate comprises data specifying a second public key of a target key pair"), an authentication code ("generating a user prompt for said authentication code") and the generation of a digital certificate only if a reply received in response to a user prompt is determined to correctly specify the authentication code ("generating said digital certificate utilizing said first private key only if said reply is determined to correctly specify said authentication code") (Applicants' claim 17, emphasis supplied). Moreover, Applicants have attempted to more clearly distinguish a "certificate" as recited in claims 1 and 17 from other elements used in conjunction with the asymmetric or public key infrastructure such as the "certified programs" taught by ***Arnold*** as will be described herein.

What Arnold Teaches

Arnold teaches a method and apparatus for protecting application data in secure storage areas (***Arnold***, Title). This protection is accomplished according to the teaching of ***Arnold*** via the creation of certified programs, the association of certified programs with persistent application data that they own, and the prevention of other applications (certified or otherwise) from accessing persistent application data not owned by them (***Arnold***, Abstract).

A certified program object is generated, according to the teaching of ***Arnold*** (see, e.g., ***Arnold***, Fig. 3), by selecting a unique program name for an application program which will be permanently associated with a persistent data area(s) owned by that application program. The program name is then combined with the actual application program into a single continuous data object block (***Arnold***, Fig. 3, block 207). A digital signature is then formed via the calculation of a hash over the data object block (***Arnold***, Fig. 3, block 211) followed by the encryption of the hashed value (***Arnold***, Fig. 3, block 215). The digital signature is then attached to the combined program/name object to form the certified program (***Arnold***, Fig. 3, block 217). It will be noted that according to this teaching, only a single public/private key pair is used (***Arnold***, Column 5, Lines 11-50).

Arnold further teaches that when a certified program is loaded by an operating system, the application program and program name are verified as being authentic by verifying the digital signature portion of the certified program. This verification process is taught by ***Arnold*** as including (see, e.g., ***Arnold***, Fig. 4) a separation of program/name data object block from the digital signature portion of the certified program (***Arnold***, Fig. 4, block 301). Once separated, the calculation of a hash is performed over the data object block and a decryption of the digital signature using the public key of the single public/private key pair (***Arnold***, Fig. 4, blocks 305 and 303, respectively). The results of these two operations are then compared to determine the authenticity of the certified program (***Arnold***, Fig. 4, block 307). Specifically, ***Arnold*** teaches that, if the two results are found to be identical, "the digital signature verifies and proves that P_A N_A was signed by the certifying authority and it also proves that P_A N_A has not been modified." (***Arnold***, Column 6, Lines 9-11). Once verified, the program name may either be associated with

a new persistent data area or used to ensure that only the application program "owning" an existing persistent data area may access it (see ***Arnold***, Column 6, Lines 24-40).

What Arnold Fails to Teach

In the present Office Action, with regard to Applicants' previously-pending claim 1, the Examiner states that at Column 5, Lines 30-42 ***Arnold*** teaches, "Establishing a master key pair including a master private key and a master public key, where a private key pair and public key pair are established" (emphasis supplied). Applicants respectfully disagree and submit that ***Arnold*** fails to teach distinct first and second public keys as recited in Applicants' claims. Applicants' claim 17, as submitted herein, recites a digital certificate generated utilizing a first private key of a master key pair including first public key and comprising data specifying a second public key of a target key pair. By contrast, ***Arnold*** teaches, as described herein, a certified program including 1) a data object block consisting of an application program and a program name and 2) a digital signature calculated from the data object block using a single key pair, K_{PR} and K_{PU}. Applicants submit that neither a digital signature, an application program, program name (or a combination thereof) of ***Arnold*** teach "a second public key" or a target key pair as claimed.

In the present Office Action, with regard to Applicants' previously-pending claim 1, the Examiner further states that ***Arnold*** teaches, "Supplying a target public key, where the public key is supplied when the keys are established." Applicants respectfully disagree for at least the foregoing reasons. Moreover, Applicants note that the present Office Action fails to indicate which portion of ***Arnold*** teaches the indicated claim element as required by 37 C.F.R. §1.104 and consequently that a *prima facie* case of anticipation has not been established with respect to Applicants' claims.

In the present Office Action, with regard to Applicants' previously-pending claim 1, the Examiner also states that ***Arnold*** teaches, "Requesting generation of a self-verifying certificate, where generation of a self verifying certificate occurs when a program asks the operating system to allocate a new persistent data area." Applicants respectfully disagree. As ***Arnold*** fails to teach distinct key pairs (and associated public keys), Applicants submit that the Examiner's

reference may not be construed as teaching a certificate which is generated utilizing a first private key of a master key pair including first public key and comprising data specifying a second public key of a target key pair as claimed. This distinction between a "certificate" as claimed by Applicants and a certified program as taught by ***Arnold*** is further highlighted numerous times within the present Application. For example, Applicants' specification states that,

> Digital certificates link details about an individual, or an organization to a public key, and are able to identify individuals, or organizations. A common use of a digital certificate is to verify that a user sending a message is the person the user claims to be. The digital certificate may contain your name, a serial number, expiration dates, a copy of the certificate holder's public key, and the digital signature of a Certificate Authority. The digital certificate contains the digital signature of the CA so that anyone can verify that the certificate is real. (Applicants' Specification, Page 3, Lines 14-24, emphasis supplied)

and further at Page 15, Lines 10-12 that, "This target key pair is different from the master key pair. The target key pair is a second, completely separate, key pair."

Applicants further submit that even if a certified program was assumed *arguendo* to teach a certificate as claimed, a certified program is not generated (or requested to be generated) according to the teaching of ***Arnold*** "when a program asks the operating system to allocate a new persistent data area" as proposed in the present Office Action. Rather, a program is certified (i.e., a certified program is generated), according to ***Arnold***'s teaching, before an application program is loaded and used (***Arnold***, Column 5, Lines 11-16). Moreover, Applicants note that the present Office Action fails to indicate which portion of ***Arnold*** teaches the indicated claim element as required by 37 C.F.R. §1.104 and accordingly that a *prima facie* case of anticipation has not been established with respect to Applicants' claims.

In the present Office Action, with regard to Applicants' previously-pending claim 1, the Examiner states that Column 5, Line 65 - Column 6, Lines 5 of ***Arnold*** teaches, "Generating a self-verifying certificate utilizing said target public key and said master key pair only in response to a correct entry of said authentication code, said certificate used only internally within said computer system, where the certificate is recovered or "generated" from the validation of the signature." The Examiner further states that ***Arnold***'s program name element teaches an "authentication code" as claimed. Applicants respectfully disagree and submit both that 1)

neither a certified program as taught by ***Arnold*** nor a certificate as claimed by Applicants is "generated" by the validation of ***Arnold***'s digital signature and further that 2) a certified program is not generated, according to ***Arnold***'s teaching, only if a reply to a user prompt is determined to correctly specify a stored authentication code as claimed.

In contradiction to the Examiner's proposed interpretation, ***Arnold*** actually teaches the inverse of the certification process (by which a certified program is created) when a certified program is verified for authenticity. For example, block 207 of Fig. 3 of ***Arnold*** "combine" as compared to block 301 of Fig. 4 "separate" illustrates this inverse relationship. Consequently, Applicants submit that a certified program is not "generated" when its component digital signature is validated. Moreover, although a program name is selected when a certified program is generated, the creation of a certified program is not contingent upon a determination that a selected program name correctly specifies a program name store elsewhere. Rather, ***Arnold***'s teaching is actually contrary to this, stating, "The name does not have to possess any special characteristics but only has to be unique within the domain of names of programs that will be certified by this particular authority" (***Arnold***, Column 5, Lines 18-21, emphasis supplied). Accordingly, Applicants submit that ***Arnold*** fails to that a certified program is generated only if a reply to a user prompt is determined to correctly specify an authentication code as required by Applicants' claims.

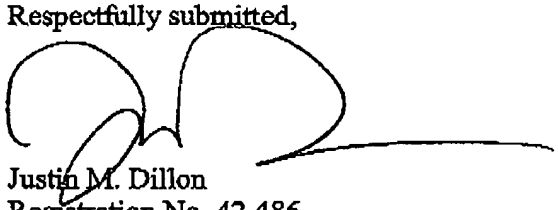
For at least the foregoing reasons, Applicants respectfully submit that claim 17, as submitted herein, is allowable in view of the Examiner's cited reference ***Arnold***. Applicants' claims 23 and 29 each include one or more elements substantially similar to those described with respect to claim 17 and are therefore allowable for at least the reasons stated with respect to that claim. All remaining claims depend directly or indirectly from Applicants' claims 17, 23 or 29 and are therefore similarly allowable.

CONCLUSION

In light of the amendments and remarks made herein, Applicants submit that all pending claims are allowable and request a Notice of Allowance thereof.

No extension of time for this response is believed to be necessary. However, in the event an extension of time is required, that extension of time is hereby requested. Please charge any fee associated with an extension of time as well as any other fee necessary to further the prosecution of this application to **IBM CORPORATION DEPOSIT ACCOUNT No. 50-0563.**

Respectfully submitted,



Justin M. Dillon
Registration No. 42,486
DILLON & YUDELL LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512.343.6116

ATTORNEY FOR APPLICANT(S)